A New Satellite Constellation Networking Certification and Reliable Maintenance Protocol(DISA)

1st Congyu Huang
School of Computer Science
Beijing Institute of Technology
Beijing, China
Email:2120171018@bit.edu.cn

2nd Liehuang Zhu
School of Computer Science
Beijing Institute of Technology
Beijing, China
Email:liehuangz@bit.edu.cn

3rd Chunlei Li
China TravelSky Holding Company
Beijing, China
Email: lcl@travelsky.com

4th Chuan Zhang
School of Computer Science
Beijing Institute of Technology
Beijing, China
Email:chuanz@bit.edu.cn

5th Yuxin Chen
School of Computer Science
Beijing Institute of Technology
Beijing, China
Email:realcyx@126.com

6thZijian Zhang
School of Computer Science
Beijing Institute of Technology
Beijing, China
Email:zhangzijian@bit.edu.cn

Abstract—With the rapid development of satellite technology, the deployment of intensive service applications through satellite has become a trend.In the process of establishing a satellite communication system, there will be some security threats such as counterfeiting, forgery, tampering.This must establish a secure satellite communication system. In this paper, according to the characteristics of satellite communication system, a protocol of satellite network authentication and trusted maintenance is designed.The protocol can accomplish two-way authentication between entities in the satellite network and the credible maintenance of the communication link. The protocol is based on the symmetric encryption system and can adapt to the current satellite load is small, the computing power is limited.This paper also analyses the security of the protocol and can resist replay attacks and man-in-the-middle attacks. Experiments show that the proposed network authentication protocol is 28% faster than the symmetric encryption system. The average time to keep the agreement credible is 254.64 ms.

Index Terms—Protocols, Security authentication, Reliable maintenance,GEO/LEO satellite networks

I. Introduction

With the continuous progress of science and technology,satellite communication system such as the Iridium system and the Globalstar system are becoming more and more popular.In those systems,satellite provide a wide range of significant services,including Weather forecasting,TV signal transmitting,global positioning,communicating and Internet accessing,etc [1]–[4].Nowadays,the satellite can provide more and more services and the satellite network is more and more perfect. It is an inevitable trend to deploy data intensive services based application in satellite,so we need to build a robust network.

Meanwhile,in satellite networks,one of the biggest challenges is how to work more securely over the network.The satellite network has the characteristics of open channel, large transmission delay, intermittent link connection and so on [5]–[7].These characteristics determine that satellite networks are more vulnerable to counterfeiting, tampering and other security threats than traditional networks.How to resist these security threats has become an important research direction.A simplest way is to authenticate network entities and users.

In order to build a robust and security network,many scholars have proposed many solutions to improve the security and robustness of satellite networks.There are some protocols guaranteed the security and some strategies provide robustness in present satellite network.Reference [8] propose a public key cryptosystem-based authentication technology.However,the authentication technology is unidirectional and can not meet the current need for bidirectional authentication.Reference [9] design and implement a two-way authentication protocol between the client and the satellite,but the authentication protocol has high maintenance cost and high failure risk.Reference [10] put forward a double-layered inclined orbit constellation to improve the robustness of satellite communication network.But they do not consider about security in the network.

We believe that this paper makes the following contributions:

(1)This paper proposes a satellite constellation network authentication protocol for double-layered satellite constellation.The network authentication protocol takes into account the characteristics of the satellites,and the

Foundation Items: The National Key Research and Development Program of China(2016YFB0800301)

DOI reference number: 10.18293/SEKE2018-041

satellite will be carried out one by one,and the satellites will be gradually authenticated by the network.

(2)This paper presents a reliable maintenance protocol,which uses geostationary-earth-orbit(GEO) satellites to control low-earth-orbit(LEO) satellite clusters, and realizes operations such as key renewal and revocation for LEO satellites under link connectivity. It ensures reliable communication and reliability of low orbit satellites.

(3)In this paper,we have analysed the security of the network authentication protocol and the security of the reliable maintenance protocol.Afterwards,we realizes the satellite network protocol and the trusted maintenance protocol by experimental simulation.In the network authentication protocol, we compare with the traditional public key system and symmetric system, the efficiency of the network authentication protocol in this paper account for 28% which is faster than original symmetric system.

II. Related Work

A. Security Authentication Protocol for Satellite Network

Zhibo,X et al. [11] put forward an end-to-end authentication protocol for satellite networks based on the Internet key exchange(IKE) protocol. The protocol is based on the IKE protocol and IKE is based on the public key encryption system. The calculation cost is high and the number of key negotiation interactions is more frequently.

Chang et al. [12] propose an authentication and key agreement protocol for satellite communications,this protocol is mainly about the authentication security between users and satellite.The protocol is not suitable for the direct use of authentication between satellites.

B. Satellite Network Reliable maintenance

X Jin et al. [13] propose a communication framework between satellite and ground station in order to improve the robustness of satellite network.Meanwhile,propose a communication architecture of space ground integrated information network which adopt simplified IP protocol, and analyse the feasibility of the implementation is analysed from the view of business process.But this framework does not consider about the communication security.

Kimura et al. [14] propose a double-layered inclined orbit constellation for satellite communication network connected by optical inter-satellite links.But this architecture is not secure because it does not take into account that will be attacked during the link transfer process. The security of information transmission in the link will be threatened greatly.

III. Satellite Constellation Network Authentication and Reliable Maintenance Protocol

Satellite network models include user terminals(UT), ground control center(GCC) and GEO satellite constellation networks, as well as LEO satellite constellation networks.Due to the need for network authentication between GEO satellites, we need to design onboard network authentication protocol to adapt the actual situation of GEO satellites.since the existence of LEO satellite networks in the system, many LEO satellites can not be directly connected with GCC because of the characteristics of LEO satellite networks. Therefore, it is necessary to study the adaptive and trustworthy link of links in resource-limited environments.In order to formally describe the model of the program, the program first establishes the model as follows.

The model of the satellite network is shown in Fig. 1.

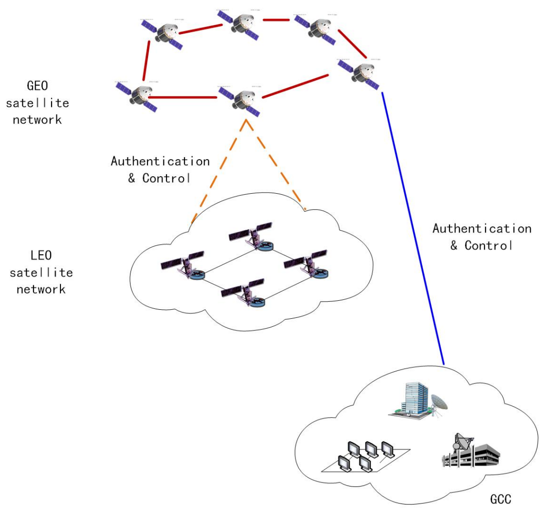

Fig. 1. Satellite network models

- GEO satellite network.GSN indicates the GEO satellite network, which consists of GEO satellites and GEO satellite links. The GEO satellite network can be represented by an undirected graph $GSN = (GV, GE)$, where GV represents a GEO satellite node like vertex in graph and GE represents a GEO satellite link like edge in graph.
- GEO satellite node.GV indicates the GEO satellite in a GEO satellite network and it is denoted as $n^{GV}, s^{GV}, c^{GV} >$, where n^{GV} Satellites node number, uniquely identifies a GEO satellite; s^{GV} is a security attribute that indicates satellite-mounted authentication information and protocols. c^{GV} indicates control information used to control LEO satellites.
- LEO satellite node.LV is a LEO satellite, and it is also possible to have a number, security attribute, and control attribute, denoted as $< n^{LV}, s^{LV}, c^{LV} >$.

The model is mainly used to achieve GEO satellite network authentication and credible maintenance.In this model, a high-orbit satellite, GV, is launched in turn. Based on the satellite security attribute s^{GV} on the GV, mutual authentication of GEO satellites and GCC can be achieved by selecting the satellite and ground authentication mode. If the certification is successful, the GEO satellite can access GCC and GCC can control the

GEO satellite and distribute the key. If the authentication fails, GCC denies access and the GEO satellite refuses the control.

After launching GV, the satellite security attribute module s^{GV} is used to select inter-satellite authentication. If the satellite authentication is successful, then a secure communication link is established between GV, whereas the two satellites can not communicate with each other. All GV satellite between the realization of the certification, all high-orbiting satellites in mutual authentication, the realization of GV networking completed GSN build.

In addition, for the LEO satellite network, due to the relatively high-speed trajectory of LV, it is difficult for GCC to control it directly.To achieve the credible maintenance of the system, GV needs to support the control of LV achieve credible maintenance.In order to achieve the security of control, it should be authenticated between GV and LV, and use the GV security attribute s^{GV}, and the type options are GV and LV. If the authentication succeeds, the control channel will establish, and GV can control LV through the secure channel, otherwise, it can not be controlled.

A. Satellite Constellation Network Authentication

1) Satellite and GCC networking Authentication: Based on the definition in the abstract model, we know that the high-orbit satellite GV is $< n^{GV}, g^{GV}, s^{GV}, c^{GV} >$.Before launching of the satellite satellite numbering, in accordance with the launch of the satellite numbering, may wish to set $G1, G2, ..., GM$.Need to set security attributes satellites, security attributes need to be defined cryptographic algorithms, keys and authentication protocols.

GEO satellites carry all the symmetric keys with LEO satellites, and the satellites use pairs of keys for authentication. Due to the limited computing power of satellites, the authentication protocol is based on a symmetric key design. The former satellite carries the symmetry K_{G_i} for itself and the control center, presets the symmetric key $K_{G_{ij}}$ used for authentication between the satellites. The original satellite sends the symmetric key to the satellite already in orbit, afterwards the satellite uses the key $K_{G_{ij}}$ for satellite authentication.

2) Authentication between GEO Satellites: Because the satellites need to be launched one by one in the process of satellite, that is, in the process of satellite networking, the satellite needs to be gradually accessed to the network, so in this process, the certification of satellites is different. When launching the first satellite, space satellites have not been networked yet. At this moment, the satellite authentication is authenticated based on the key set in advance. After the first one is authenticated, the satellite of the second backbone network is deployed and controlled K_{G_1} for center certification, and $K_{G_{12}}$ and SQN sequences for the first and second satellite certifications.

First of all, it is determined whether the inter-satellite certification link can be constructed with the adjacent satellites. If an inter-satellite certification link can be constructed, the first and second inter-satellite authentication can be established by using the secure communication channel between the network service center and the previous satellite. The symmetric key $K_{G_{12}}$ and the SQN sequence are sent to the first satellite so that both the first satellite and the second satellite have the authentication key $K_{G_{12}}$ and the SQN sequence. The specific process of certification is shown in Fig. 2. The process behind the satellite is similar. After all the satellites are launched, a high-orbit satellite network is established between the satellites, thus completing the satellite networking Authentication process.

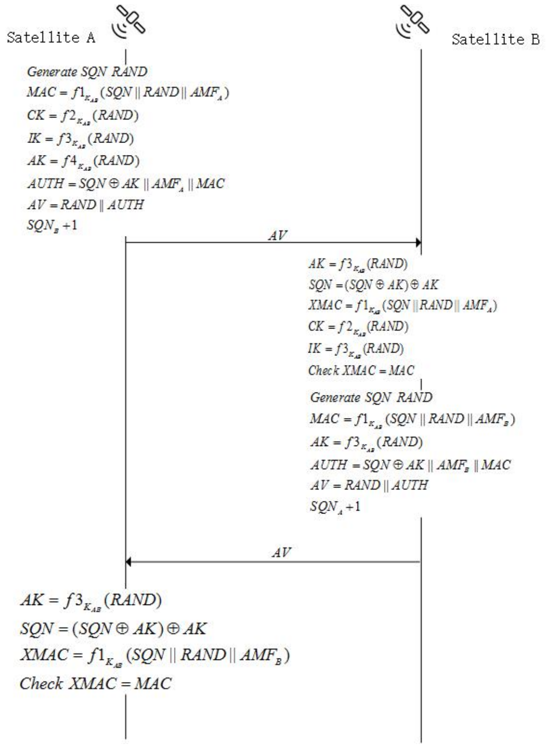

Fig. 2. Authentication between Satellites

(1)First,satellite A sends an authentication request message to satellite B.Before the satellite A initiates the authentication request, it needs to calculate the authentication vector AV based on its own key K_{AB}, where the authentication vector consists of the following three elements, namely the random number $RAND$, the session key for encryption CK, authentication token AUTH.Each vector AV generation process is as follows. Generate sequence number SQN and random number RAND, and calculate $MAC = f1_{K_{AB}}(SQN||RAND)\ CK = f2_{K_{AB}}(RAND)\ AK = f3_{K_{AB}}(RAND)\ AUTH = SQN \oplus AK||MAC\ AV = RAND||AUTH$.Satellite A then sends the vector AV to satellite B.

(2)After satellite B receives the AV from satellite A, satellite B calculates AK using K_{AB} through RAND, decrypts it with AK to obtain SQN and verifies whether satellite A is valid by computing $f1_{K_{AB}}(SQN||RAND)$ Has a symmetric key K_{AB}.After the verification is passed, a new random number $RAND$ is generated and calculates $MAC = f1_{K_{AB}}(SQN||RAND)$ $CK = f2_{K_{AB}}(RAND)$ $AK = f3_{K_{AB}}(RAND)$ $AUTH = SQN \oplus AK||MAC$ $AV = RAND||AUTH$.Then sent the vector AV to satellite A.

(3)After satellite B's AV is received by satellite A, AK is computed by RAND using K_{AB} and decrypted by AK to obtain SQN, verifying whether satellite B is valid by computing $f1_{K_{AB}}(SQN||RAND)$ Have a symmetric key K_{AB}, verify the success, then the certification process is completed.

In the algorithm, the function $f1$ used as a message verification code generation function, and $f2$ and $f3$ are key derivation functions [15].

B. Reliable Maintenance

The main needs of GEO satellites for reliable maintenance of LEO satellites are divided into two steps. The first step is to authenticate connection between the GEO satellites and the LEO satellites. The second step is to control the LEO satellites by using the control attributes of the GEO satellites.

1) Authentication between GEO satellite and LEO satellite: After GEO satellite network and LEO satellite network set up to achieve double-layer satellite networking, access authentication is achieved through LEO satellite network, and backup and trusted maintenance is achieved through GEO satellite network.

In the current international environment, basically all countries can not be deployed on a global scale.When satellite authentication systems need to be updated, there is no guarantee that all satellite satellites will be able to travel through one country, which may result in a failure to update all of them during the update. In this case, GEO satellites are required to cover the LEO satellites.

After the completion of the construction of the double-layer network, it is also necessary to consider the process of completing the certification of the LEO satellites and the LEO satellites during use. The certification process between LEO and LEO satellites is similar to the process of certification between GEO and GEO satellites, as detailed in the earlier section on certification between GEO satellites.

The reliable maintenance of the GEO satellite network for the LEO satellite network is to update the authentication module, such as the authentication key in the system of the LEO satellite network.When a satellite is out of work,the packets that were originally forwarded through the failed satellite will no longer pass the invalid satellite.At this time, we need to broadcast the entire network to the failed satellites in the LEO satellite network by the high orbit satellite, which will make the related topological paths of the failed satellites change to infinity,indicating that the other satellites which satellite is failed, and will invalidate the failed satellite's authentication key.The process is shown in Fig. 3.

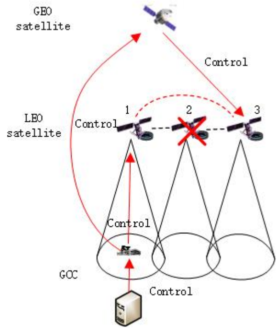

Fig. 3. Control the invalid LEO satellite

The following example illustrates the failure of a high-orbiting satellite to describe the process of updating keys and reestablishing a secure communication channel between adjacent high-satellites after symmetric key deletion. The process is shown in Fig. 4.

(1)For authentication between satellite and GCC, we use 3GPP's authentication protocol [15]. The satellite A and GCC are authenticated and the session key CK_1 and the integrity key IK_1 are obtained. The satellite B and GCC are authenticated and the session key CK_2 and the integrity key IK_2 are obtained. After completing the above process, two satellites and GCC secure communication channels are established.

(2)The GCC assigns the symmetric keys K_{AB} and ID_B to the satellite A through the secure channel. At the same time, the GCC secure channel allocates the symmetric keys K_{AB} and ID_A to the satellite B.

(3)Satellite A and satellite B complete the certification. For details on the authentication method, see Satellite Constellation Network Authentication Section.

The completion of the above steps will enable the implementation of satellite key update and reliable maintenance.

IV. Security Analysis and Performance Analysis

A. Security Analysis

In the satellite network authentication protocol, the protocol can accomplish two or two-way satellite authentication. The protocol used is based on the 3GPP protocol and uses symmetric keys to ensure the privacy of the protocol. The protocol uses message authentication codes to ensure the integrity of information during transmission, thus being able to resist attacks such as counterfeiting and forgery. Due to the large transmission delay of the satellite, the use of timestamps to resist replay attacks is less controllable. We use the serial number SQN instead of timestamps to protect against replay attacks. In the

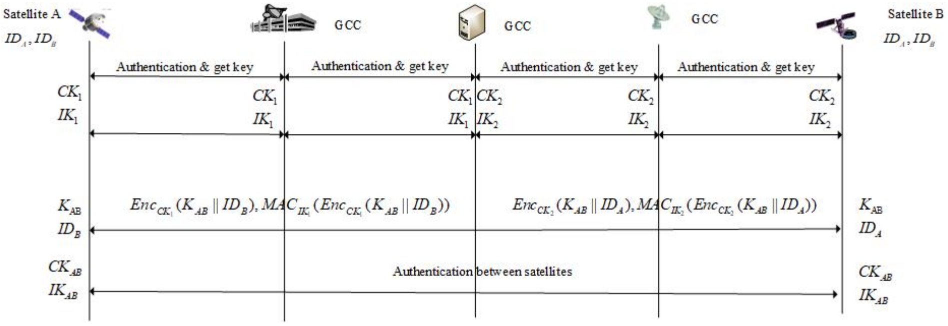

Fig. 4. Control the invalid LEO satellite protocol

process of satellite communication, key transmission is established in the secure channel, which can effectively resist man-in-the-middle attacks.

In the reliable maintenance protocol, the control link first passes two-way authentication and generates the session key and the integrity key. This ensures the privacy and completeness of the process of transmitting the update key in the control link. During the process of re-establishing the link, the protocol derives the symmetric authentication key and integrity key using the symmetric key derivation function to protect the underlying symmetric key to ensure the privacy and integrity of the protocol. Through the above two methods, it can resist attacks such as counterfeiting and counterfeiting in the satellite environment. The agreement also uses the serial number SQN to resist replay attacks.

B. Performance Analysis

In order to test the performance of the protocol, the protocol was simulated to analyze the performance under an Intel (R) Core i7-7700HQ CPU@2.80GHz processor. Respectively, the network authentication protocol and trusted to keep the agreement has been tested. This experiment uses openssl open source library security algorithm for experiments.

In this paper, 100 tests of network authentication were conducted and compared with the traditional symmetry scheme, the test results shown in Fig.5. Due to the large satellite delay, we removed the satellite communication delay and compared the calculation times of the two authentication schemes. The protocol calculation time is shown in Fig. 6.

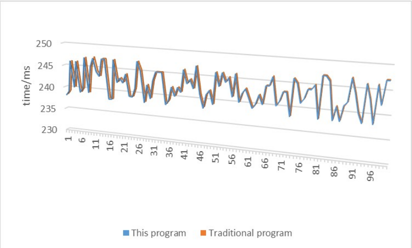

Fig. 5. Network authentication performance test results

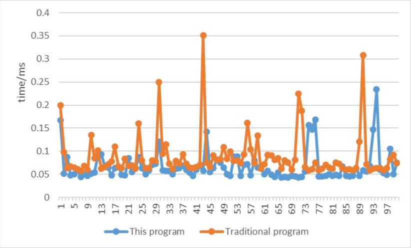

Fig. 6. Protocol calculation time

In the experimental results, the maximum calculation time of this scheme is 0.339 ms , the minimum time is 0.048 ms and the average calculation time is 0.074 ms. The maximum calculation time of the the traditional symmetry authentication scheme is 0.289 ms ,the minimum calculation time is 0.061 ms and the average calculation time is 0.093 ms. The average efficiency of this scheme is 28% higher than that of public key encryption schemes.

This article also tests the trusted maintenance for 10 times, and the test results are shown in figure 7. As the satellite failure increases, the test results are shown in figure 8.

The experimental results, the maximum time of this program for reliable maintenance is 272.14 ms, the minimum time is 238.20 ms, the average time is 254.64 ms.

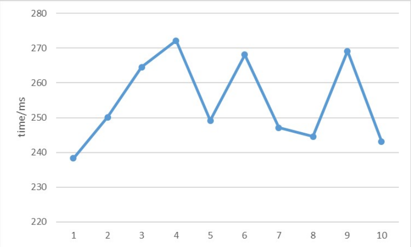

Fig. 7. Reliable maintenance of test results

V. Conclusion

This paper designs a new GEO satellite network authentication and credible maintenance protocol, verifies the feasibility and efficiency of the protocol experimentally,

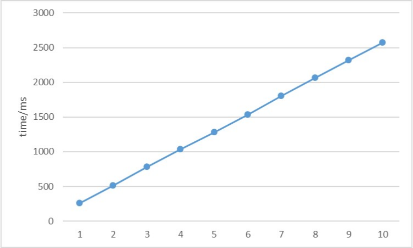

Fig. 8. Failure satellite increasing test results

and proves the security of the protocol through theoretical analysis.

Future satellite computing power will be more and more strong, the use of public key system on the satellite will be the new direction. For credible maintenance of LEO satellites, other safer and more efficient options may emerge in the future.

References

[1] Amirshahi, Pouyan, and Steven Grippando. ”Radio frequency interference monitoring system for weather satellite ground stations: Challenges and opportunities.” Dynamic Spectrum Access Networks (DySPAN), 2017 IEEE International Symposium on. IEEE, 2017.

[2] Berman, Elliot. ”Movable window support device for a satellite TV dish.” U.S. Patent No. 6,731,250. 4 May 2004.

[3] De Sanctis, Mauro, et al. ”Satellite communications supporting internet of remote things.” IEEE Internet of Things Journal 3.1 (2016): 113-123.

[4] Ashjaee, Javad, et al. ”Satellite differential positioning receiver using multiple base-rover antennas.” U.S. Patent No. 9,035,826. 19 May 2015.

[5] LI F H , YIN L H , WU W ,et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016,37(11): 156-168.

[6] Jiang, Chunxiao, et al. ”Security in space information networks.” IEEE communications magazine 53.8 (2015): 82-88. Zheng, Gan, Pantelis-Daniel Arapoglou, and Bjorn Ottersten.

[7] ”Physical layer security in multibeam satellite systems.” IEEE Transactions on wireless communications 11.2 (2012): 852-863.

[8] Wullems C, Pozzobon O, Kubik K. Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems[C]// European Navigation Conference Gnss. 2005:1.

[9] Cruickshank H S. A security system for satellite networks. Proceedings of the Fifth International Conference on Satellite Systems for Mobile Communications and Navigation, London, UK, 1996.

[10] Sasaki, Takao, and Tadayoshi Katoh. ”Dual layer satellite communications system and geostationary satellite therefor.” U.S. Patent No. 6,023,605. 8 Feb. 2000.

[11] Zhibo, X., Ma, H.: Design and simulation of security authentication protocol for satellite network. Comput. Eng. Appl. 43(17), 130–132 (2007)

[12] Chang, Chin-Chen, Ting-Fang Cheng, and Hsiao-Ling Wu. ”An authentication and key agreement protocol for satellite communications.” International Journal of Communication Systems 27.10 (2014): 1994-2006.

[13] Jin, Xiaoning, Peiying Zhang, and Haipeng Yao. ”A communication framework between backbone satellites and ground stations.” Communications and Information Technologies (ISCIT), 2016 16th International Symposium on. IEEE, 2016.

[14] Kimura, Kazuhiro, Keizo Inagaki, and Yoshio Karasawa. ”Double-layered inclined orbit constellation for advanced satellite communications network.” IEICE Transactions on Communications 80.1 (1997): 93-102.

[15] 3GPP, TS 33.102 v9.1.0. 3G Security; Security architecture (Release 9), 2009.12